DEFENCE
SCIENCE & TECHNOLOGY

DSTO

IP Convergence in Global Telecommunications - Mobility in IP Networks

Sana Jayasinghe

DSTO-TR-1393

DEFENCE
SCIENCE & TECHNOLOGY

IP Convergence in Global Telecommunications - Mobility in IP Networks

Sana Jayasinghe

Information Networks Division
Information Sciences Laboratory

DSTO-TR-1393

ABSTRACT

The paper describes the main techniques for providing mobility in an IP network. Towards this end the Mobile IP protocol is described in both its guises, namely MIPv4 and MIPv6. Fast mobility is addressed in the next section, and Cellular IP is chosen as the representative protocol. Then, the methods of providing mobility by using a cellular network is presented, and the paper concludes with the description of some common wireless standards.

RELEASE LIMITATION

Approved for public release

Published by

DSTO Information Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-012-593
February 2003

APPROVED FOR PUBLIC RELEASE

IP Convergence in Global Telecommunications - Mobility in IP Networks

Executive Summary

Since their inception, IP networks have gained in popularity to such an extent that they may now safely be considered as *de facto* standards, certainly for data communications, if not for voice. It is, thus, useful to understand the capabilities and limitations of IP networks with respect to various criteria. One such criterion is the provision of mobility. Traditionally, IP networks were designed for the interconnection of static devices, as is evident from their fundamental principles, such as their addressing structure. So, the provision of mobility, although of paramount importance, has been an afterthought. This has resulted in a multiplicity of solutions, all of them sub optimal in some sense. This paper addresses the main ways by which mobility may be incorporated in an IP network, and assesses their strengths and weaknesses.

From a military perspective, the provision of mobility greatly enhances the utility of an IP network. Consider, for example, a ship that is attached, by some wireless means, to a shore based IP network. As the ship moves around, it must change its point of attachment to the network. Under normal circumstances, this would result in configuration changes that would disrupt any applications. However, if the network provided for the mobility of the ship, then, these changes would be in the protocols operating *within* the network, and, as far the ship is concerned, there would be seamless connectivity and application transparency. The same may be said for aircraft that are trying to maintain uninterrupted connectivity with an IP network, with the proviso that, in this case, the network must address fast mobility.

This paper begins with a description of Mobile IP, the only standard for the provision of mobility in IP networks. Two versions of Mobile IP, namely MIPv4 and MIPv6, are compared and contrasted. Security issues are addressed. Then, the paper discusses micromobility, which allows for fast mobility. One of its exponents, Cellular IP, is described briefly. Finally, the paper describes ways and means of using cellular networks to provide IP mobility.

Author

Sana Jayasinghe
Information Networks Division

Sana Jayasinghe graduated with a B.Sc. Honours in Electronic, Computer and Systems Engineering from Loughborough University of Technology in 1983. His Ph.D. was awarded from the same university in 1989. After working as a research fellow for a short while, he joined DSTO in 1991. His current research interests are in IP networks, wireless systems, and ad hoc networks.

Contents

1. Introduction

One of the key features of the information technology revolution is that there has been a continuous increase in the power of small computers. The notebooks, laptops and personal digital assistants of the current generation can boast even greater power than the early mainframes. Hence, the demand for these small computers has seen an exponential growth, fuelled not only by the increase in power, but also by the reduction in price. However, power and price notwithstanding, one of the main drivers for this growth in demand is the potential for mobility afforded by these devices. The reality of the 'anytime, anywhere' concept has been widely embraced, making mobility an important attribute in the scheme of things.

Inherent in the attribute of mobility is the concept of connectivity. Consumers now demand that an external entity can be reached via their mobile devices. Thus, these mobile devices have become part of a network. There are two paradigms here, that of mobile telephony, and that of mobile computing. In mobile telephony, the main service is the delivery of voice. Mobile phones are connected to a cellular network which is, in general, a circuit switched network optimised for voice communications. Although the transmission of data is possible, it is of secondary concern in these networks. The complete opposite is true of mobile computing. In mobile computing, the devices are connected to networks which are packet switched, and thereby optimised for data transmission. Layered communications is essential in these networks. Most of these networks obey the Internet Protocol in the network layer, and as such, are known as IP networks, of which the Internet is a prime example. This paper is concerned mainly with the issue of mobility in IP networks.

One of the issues concerned with the provision of mobility is that the application should be completely unaware that the host is mobile. Thus, the protocols that provide mobility should reside in the lower layers. Given that the physical layer is hardware oriented, the lowest layer that mobility protocols may reside in is the link layer. However, this is not optimum since the system would then be link layer dependent. For example, if a cellular network were to provide mobility at the link layer, the service could be enjoyed only within the cellular network. This has two disadvantages. Firstly, the service can only be obtained within the coverage area of the cellular network. Secondly, if there was another network with superior characteristics available (such as an 802.11 wireless LAN), the user cannot switch to this due to the dependence on the cellular link layer. If, however, the mobility protocol were to reside in the network layer, it would be independent of the link layer, and the user could roam across heterogeneous networks in order to obtain a service that was optimum in some sense. Thus the optimum condition is for the mobility protocol to reside in the network layer. There are quite a few protocols that have been designed to do this but only one of them has been standardised by the Internet Engineering Task Force (IETF). This protocol is called Mobile IP [1-2]. The fact that this is the standard protocol for the provision of mobility in IP networks means that vendors will opt to implement this, rather than any other protocol. This has indeed been the case, and currently there are

many implementations of Mobile IP. This paper gives the operation of Mobile IP and describes its closely related issues.

Although Mobile IP is an IETF standard, it is not without limitations. In particular, as a mobile host changes its point of attachment to an IP network, Mobile IP instigates a registration procedure which may be relatively time consuming. This adversely affects any mobile host that changes its point of attachment frequently, such as could be the case for a person using a computer on a high speed train travelling through a metropolitan area. Thus, Mobile IP does not perform very well in the presence of fast handoffs. There are other protocols that have been designed to service fast handoffs, and coexist with Mobile IP. Cellular IP, Hawaii, and Thema are three such protocols, and this paper describes Cellular IP [3] briefly, in order that the reader may gain some understanding on this issue.

The discussion in this paper so far, has been centred on mobile computing in the presence of IP networks. However, it is informative, at this stage, to broaden the perspective and consider related issues pertaining to cellular networks. The reason for this is that although cellular networks were originally meant mainly for voice communications, they are being modified (or value added) to support data transmission as well. In other words, from a networking perspective, the boundaries between mobile telephony and mobile computing are becoming blurred. Furthermore, there is much discussion on using IP in cellular networks. This being the case, the paper discusses some protocols that have been used for data transmission in cellular networks, and finally, introduces some related, proposed wireless standards.

2. Mobile IP

All IP networks have a hierarchical addressing structure. The first portion of the address defines the subnet to which the host belongs, and the last portion of the address defines the host itself. Thus, the addressing is location dependent. So, if a host moves and changes the subnet to which it is attached, then, under normal circumstances, it must change the IP address in order to continue communications. Changing the IP address means altering other configuration settings as well, so any application that was running would have been disrupted. Mobile IP is a protocol that solves this problem by letting mobile hosts move around without changing their IP addresses.

Lets reiterate. What is the functionality of Mobile IP? Simply stated, it allows for continuous communications as a mobile host moves around an IP wide area network and changes its point of attachment to the network. The mobile host does not have to change its IP address as it changes its point of attachment to the network. Mobile IP provides application transparency and seamless roaming. Application transparency is that the applications need not be mobile aware and would continue to run without any disruption as the mobile host moves around. Seamless roaming allows the mobile host to attach itself to foreign IP networks (networks whose network prefixes are different to that of the mobile hosts) and still maintain communications without the need to change its IP address.

At this stage, the alert reader may complain that this functionality can be provided by using the Dynamic Host Configuration Protocol (DHCP). For example, if a mobile host changes its point of attachment, it may request a DHCP server to assign it a new IP address. This is quite correct except that the mobile node has to undergo a change in its IP address and therefore some disruption to the application. So, although DHCP will solve the problem with respect to portable hosts, it cannot service truly mobile hosts. Mobile IP, on the other hand, does not require changes in IP addresses, and therefore will maintain communications in the presence of mobility as well as portability.

Mobile IP has the ability to service mobile networks, as well as mobile hosts. Consider a patrol boat (the mobile host) that is attached, initially, to a shore based network. As it moves around, it loses connectivity with the shore based network and attaches itself to a ships LAN. Because the routing has changed it can no longer communicate unless it changes its IP address. Mobile IP circumvents this problem. The second scenario is that of a ship moving around and changing its point of attachment to an IP WAN. Note that a ship will have its own router and hosts and subnet so, in this sense it is not merely a mobile host but an entire mobile network. Mobile IP allows this movement without causing any disruption in communications.

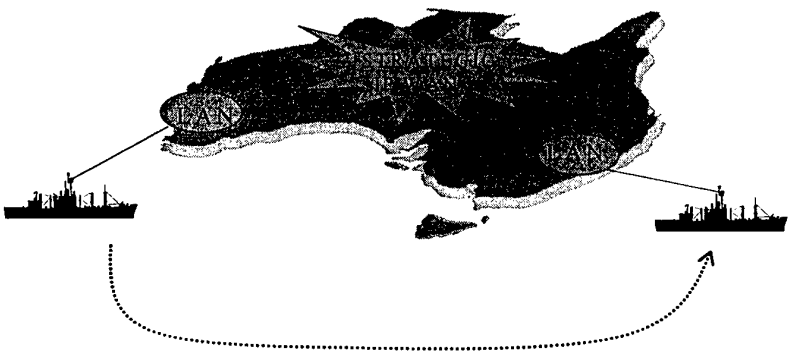

Figure 1: A scenario requiring Mobile IP

Figure 1 exemplifies the scenario of a ship requiring Mobile IP. Under normal circumstances the ship is attached to a LAN which is its home network. This could, for example, be based in Perth. The LAN itself is attached to a strategic network that uses IP as its layer 3 communications protocol. Regardless of where it originates, all communications addressed to the ship are sent to the LAN at Perth, and thence, onto the ship. Now consider the situation where the ship has to move to Sydney. It can no longer maintain connectivity with the LAN at Perth but, instead, has to attach itself to a LAN at Sydney. Unless the IP address is changed, all communications to the ship will still arrive at the LAN at Perth and thereby, will be lost, because the ship has changed its point of attachment to the IP network. Changing the IP address, albeit a possible solution, is rather cumbersome, especially if the ship has to move around often. The more elegant solution is to use Mobile IP, which caters for this movement of the ship, and still maintains continuous communications.

With the advent of the next generation IP, that is IPv6, there are two versions of mobile IP that have been specified, namely, mobile IPv4 (MIPv4) and mobile IPv6 (MIPv6). The specification of MIPv6 is still only a draft standard and there is only a single implementation that is known to the author. However, it is interesting to briefly compare and contrast MIPv4 with MIPv6, in order to ascertain the different functionalities. Towards this end, the paper gives the operation of MIPv4.

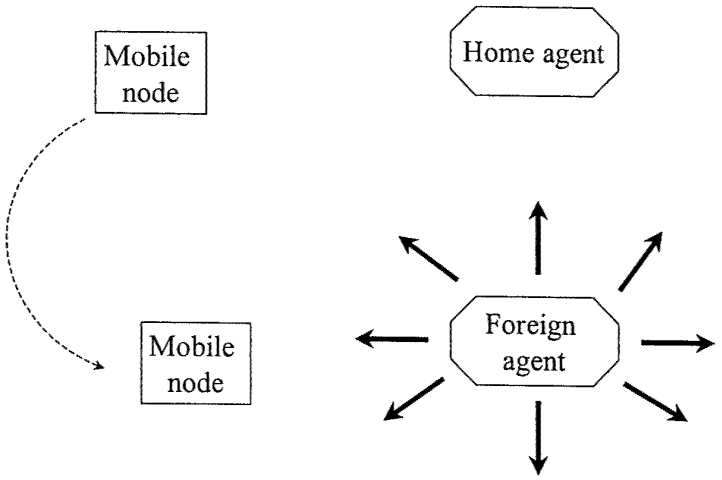

Figure 2: Agent advertisement

2.1 Mobile IPv4

Before proceeding any further, it is informative to introduce the concept of a home agent and a foreign agent, and some terminology. A mobile node in its normal location is attached to a home network. A home agent is a router on this home network, that is responsible for directing datagrams to the mobile node. When the mobile node moves, it may attach itself to other visited networks. A foreign agent is a router on any of the visited networks. It is also involved in the delivery of datagrams to the mobile node. A correspondent node is a node that wishes to communicate with the mobile node.

Mobile IPv4 can be considered to be the integration of three distinct operations. These are agent advertisement, registration, and tunneling. Figure 2 shows the process of agent advertisement. When a mobile node moves away from its home network it loses connectivity with the home agent. It must now attach itself to a visited network. To do this, it listens on the appropriate link to any messages broadcast by a foreign agent. Foreign agents are responsible for periodically broadcasting agent advertisements. The format of these advertisements is the same as the ICMP router discovery messages in normal IP, except that in agent advertisements, there are extensions. The main extension is the provision of a care-of address for use by the mobile node. Thus, the primary function of agent advertisement is for the mobile node to obtain a care-of-address via the foreign agent.

The next part of the MIPv4 protocol is registration. Figure 3 shows this process. After the mobile node has received a care-of address from the foreign agent, it must register this address with the home agent, so that the home agent will know where to redirect any packets that are addressed to the mobile node. To do this, the mobile node compiles a

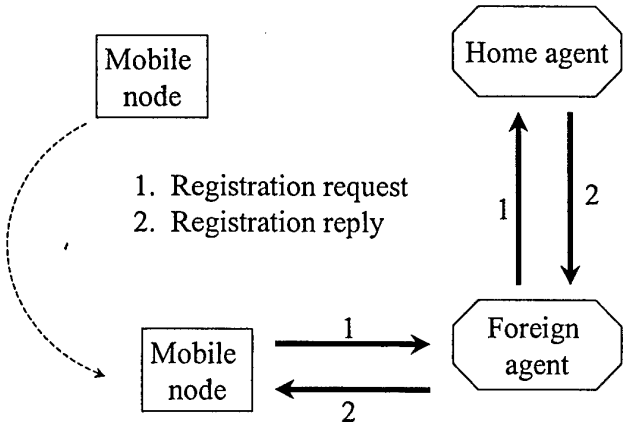

Figure 3: Registration

registration request packet and sends it, via the foreign agent, to the home agent. Upon receipt of a registration request, the home agent compiles a registration reply and sends it to the mobile node. This registration reply will either confirm or reject registration. If the registration is accepted, the mobile node has established a binding with the home agent. A binding is a triplet containing the home address, care-of address, and registration lifetime. When the registration lifetime expires, the mobile node has to reregister with the home agent, even if the foreign agent (and hence, the care-of address) has not changed. In this exchange of messages, the foreign agent acts as a passive node. Furthermore, when the mobile node returns to its home network, it must deregister with the home agent.

The final part of the basic MIPv4 protocol is tunneling. Consider the situation where a mobile node has obtained a care-of address from a foreign agent, and has registered this address with its home agent. Now, if the mobile node wants to send a packet to a

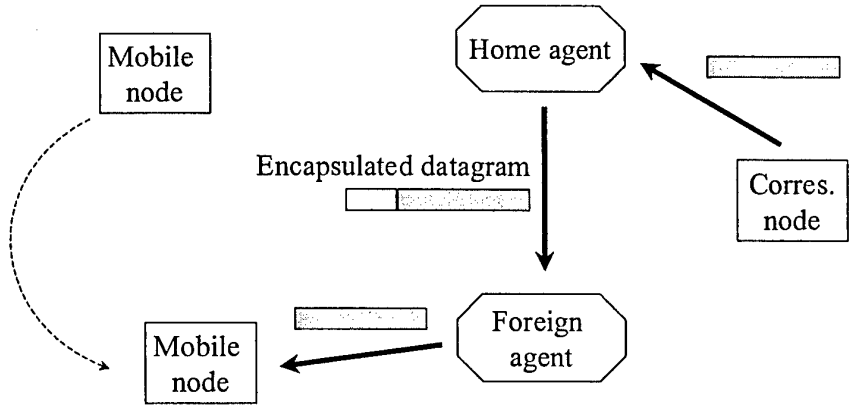

Figure 4:Tunneling

correspondent node, it places the address of the correspondent node in the IP destination address field and transmits the packet either to the foreign agent, or to a router that has previously sent a Router Advertisement (this router advertisement may have been incorporated in the earlier agent advertisement sent by the foreign agent.). From this point onwards, normal network prefix routing is used to deliver the packet to the correspondent node, and no tunneling is necessary in this case.

However, the situation is quite different in the case where a correspondent node desires to send a packet to the mobile node. In compiling the packet, the correspondent node has its own address as the source address, and the address of the mobile node as the destination address. Since the home agent has advertised reachability to the mobile node, this packet is routed, initially, to the home agent. The home agent now encapsulates this packet in an outer packet with the mobile nodes care-of address as the destination address and sends this encapsulated packet to the foreign agent. This is called tunneling. The foreign agent decapsulates and sends the original packet to the mobile node. The default encapsulation is IP-within-IP, which must be supported by all mobile nodes, home agents, and foreign agents. The fields for the new IP header are selected naturally. Other forms of encapsulation may be used if agreed to by the mobile node, home agent and foreign agent. Two of these other forms are minimal encapsulation (which uses fewer bytes per datagram), and (Generic Routing Encapsulation (GRE) encapsulation.

2.2 Mobile IPv6 comparison

In MIPv6 there are no foreign agents. The main reason for having a foreign agent in MIPv4 was to provide a care-of address to a given mobile node. This care-of address was subsequently used for routing purposes. Furthermore, since a foreign agent could service many mobile nodes with a single care-of address, this saved on the number of IP addresses that needed to be allocated to mobile nodes. This was a pleasing feature because in MIPv4, the address space, being just 2^{32}, is relatively small. Thus, if lots of nodes were mobile, there is a danger of running out of addresses. In MIPv6 there is no such problem since the address space is 2^{128}, and every mobile node could have its own care-of address.

This is exactly what happens in MIPv6. Every mobile node can obtain its own collocated care-of address via the MIPv6 features Stateless Address Autoconfiguration and Neighbour Discovery. Stateless Address Autoconfiguration is a means of obtaining an IP address automatically. No servers are involved. The mobile node first forms an interface token, which is usually its link layer address. It then obtains a network prefix via the Neighbour Discovery mechanism, and concatenates the network prefix with the interface token to give a new IP address. This method could be used to obtain care-of addresses as the mobile node changes its point of attachment to the fixed network. This completely obviates the need for foreign agents. In MIPv4, if a correspondent node wanted to communicate with a mobile node, it would have to do so via the home agent. This is because the correspondent node would have no knowledge of the location of the mobile node. This, however, causes obvious inefficiencies in routing, because, in some cases, the

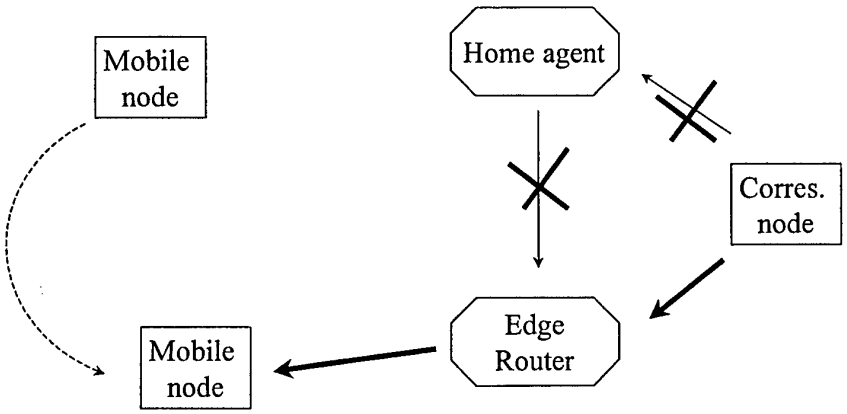

Figure 5:Route Optimization

mobile node and the correspondent node may be physically near each other, while the home agent is on a distant subnet. In MIPv6 this problem is eliminated by employing route optimization, which allows the correspondent node to send datagrams directly to the mobile node. This is shown diagrammatically in Figure5. To effect route optimization, the correspondent node has to be informed about the mobile nodes care-of address. This is done via the IPv6 extension headers. Once the correspondent node has received the care-of address of the mobile node, it can communicate directly. There is no need for tunneling of datagrams. However, for those correspondent nodes that do not know the care-of address of the mobile node, the situation is as before, with the home agent tunneling the appropriate datagrams. It should be noted here that MIPv4 also specifies route optimization, but only as an extension to the basic protocol. This means that all mobile nodes may not employ it.

Route optimization lends itself naturally to the concept of smooth handoffs. When a mobile node moves its point of attachment from one foreign network to another it must use a new care-of address. To do this, it must inform the home agent and correspondent nodes about this new care-of-address via binding updates. It is only after binding acknowledgements are received that the mobile node can be certain of the validity of the new care-of address. In this interim time, many datagrams will appear at the old care-of address, and will be discarded since the old care-of address is no longer valid.

This problem is circumvented in MIPv6 as follows. When the mobile node moves its point of attachment to the fixed network, it sends a binding update to the old router that serviced its old care-of address. This binding update associates the new care-of address with the old care-of address. The old router is now requested (via the binding update), to act as a temporary home agent for the old care-of address. This means that any datagrams addressed to the old care-of address will be redirected by the old router, to the new care-of address. Indeed, these datagrams are tunnelled to the new care-of address by the old router using IPv6 encapsulation. This happens until the bindings are established by the

mobile node, home agent and correspondent nodes, after which, the datagrams are again transmitted directly to the mobile node.

Apart from those noted above, there are other differences in the two protocols MIPv4 and MIPv6. Noting down every difference is beyond the scope of this report. However, it is perhaps clear that utilising MIPv6 is more advantageous than utilising MIPv4. But, the specification of MIPv6 is still in its infancy, and as mentioned earlier, there are not many implementations. It is therefore slightly risky, and perhaps not possible, for carriers to consider employing MIPv6 at this point in time. The better option is to consider MIPv4, and change to MIPv6 when the technology becomes slightly more mature.

2.3 Security

Although the primary functionality of Mobile IP is to provide mobility to IP hosts at the network layer, it is important that this be done in a secure manner. The main point of vulnerability in Mobile IP is the registration request. The main purpose of Figure 6

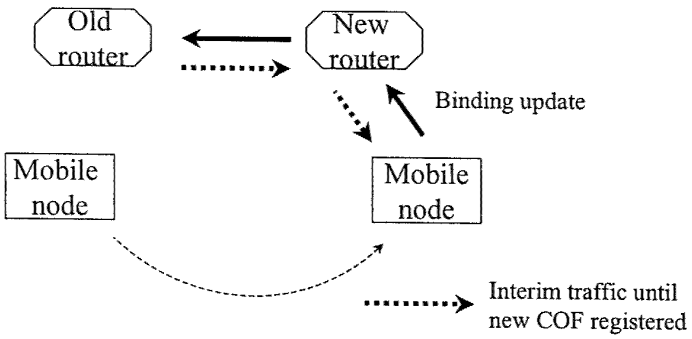

Figure 6:Smooth Handoffs

registration request is to register the mobile nodes care-of address with the home agent. Now, any malicious user could easily obtain the home address of a given mobile node since there is nothing secret in this piece of information. This user could then compile a registration request for a given mobile node with its own address as the care-of address. Once this is registered by the home agent, all subsequent communications to the mobile node would be sent to this care-of address, which, of course, is the address of the malicious user. Thus, not only has this user stopped the mobile node from receiving any datagrams, it also has succeeded in intercepting the traffic that is meant for the mobile node. Furthermore, it can create this problem from anywhere in the network, that is, it doesn't have to be in the path between the mobile node and the home agent. The problem is the same in MIPv6 because a registration request is replaced by a binding update with similar functionality in MIPv6.

Mobile IP circumvents this problem by insisting that all registration requests (and binding updates in MIPv6) be authenticated. To do this, there is a security association between the mobile node and the home agent. This security association determines the authentication

algorithm that is used and the shared secret key. The default authentication algorithm that every mobile node and home agent must use is called Keyed Message Digest 5 (MD5). In the registration request, there is a field for the authenticator, which the mobile node computes using the authentication algorithm, secret key and the data in the registration request. On receipt of this registration request, the home agent independently computes the authenticator. If the two authenticators match, then the home agent can be assured that the registration request is from a genuine mobile node, because a malicious user would not have access to the authentication algorithm and the secret key. The home agent then proceeds with sending the registration reply, which is also authenticated. Thus, authentication prevents malicious users from entering the mobile IP loop at the point of the registration request. Note that since the data in the registration is used to compute the authenticator, this process ensures that the data is correct, that is, it provides automatic data integrity checking.

While the above form of authentication stops malicious users from generating false registration requests and intercepting packets, it still does not stop a malicious user from being able to deny service to a mobile node for the following reason. A malicious user could listen for transmissions by the mobile node and store any registration requests with the intention of using them at a later time. Since the message has been compiled by the mobile node, the authenticators will match when the message is replayed at a later time by the malicious user. Of course at this later time the mobile node may have moved sufficiently to change its care-of address, in which case the care-of address in the registration request that is replayed by the malicious user (and accepted by the home agent), would be out of date, and all subsequent packets to the mobile node would be lost.

In order to prevent this from happening, the mobile IP protocol specifies an Identification field in the registration request and reply. This Identification field in the registration request contains an estimate of the current date and time as perceived by the mobile node. When the home agent receives this registration request, it checks the timestamp in the Identification field to see whether the times are sufficiently close. If not it rejects the registration request by sending the appropriate registration reply. Thus, if a malicious user replayed a genuine registration request at a later time, the timestamp would not be correct (note that the malicious user cannot change the timestamp since then the authenticators would not match due to data integrity checking) and the request would be rejected by the home agent. The only problem with this is that the mobile node and the home agent could be out of synchronisation with respect to time, in which case the registration request would be rejected since the times do not match. However, the home agent supplies enough information in the registration reply for the mobile node to synchronise the time, so that any subsequent registration requests will not contain this anomaly. Then, if the mobile node tries again, it will succeed.

2.4 Commercial implications

There are many solutions that have been proposed to solve the problem of mobility in IP networks. Among the most prominent are Mosquito Net from Stanford University and

other solutions from Harvard University and Carnegie Mellon University. However, all these solutions may be considered to be academic curiosities, when compared with Mobile IP as given above, since Mobile IP is the solution that has been standardised by the Internet Engineering Task Force (IETF). At present, Mobile IPv4 is a full standard and the specification is given in RFC 2002. Mobile IPv6 is in the process of becoming a full standard, and it is inevitable that this will happen.

It is, however, one thing to specify a protocol but quite another to implement it. Given this fact, quite a few institutions around the world have implemented Mobile IPv4. There are implementations that run on Solaris, Linux, and Windows NT platforms. For example, ikV in Germany sell home agent, foreign agent, and mobile node software that runs on Windows NT. It is also fairly cheap, with the total cost being about A$ 500. Cisco Systems have an implementation of the home agent and foreign agent that run on their routers. This implementation is interoperable with any mobile node software. Furthermore, Cisco Systems have developed mobile routers (these are specified in MIPv4), which are essential in order to make a whole network mobile (eg. ship). As regards MIPv6, there are not many implementations worldwide, with the exception of Ericsson, who tested an MIPv6 implementation recently. However, this situation is expected to change when MIPv6 becomes a full standard.

The deployment of MIPv4 in networks has initially been within academic environments. Thus, the focus has been on campus wide networks using MIPv4. A notable exception is Motorola, which uses MIPv4 in its Integrated Digital Enhanced Network (iDEN), which is a proprietary US radio network. It is expected that this situation is bound to change with Mobile IP being adopted by many institutions as the need arises. This will become especially true after the full standardisation of MIPv6 with its tighter security features. Indeed, it was mentioned at the recent IETF meeting that telecommunications companies and cellular carriers are beginning to be interested in Mobile IP, and it is expected that widespread deployment will follow when the technology is mature.

3. Micromobility

This section presents a slightly different architecture that could be used in IP networks. This architecture gives rise to the problem of handling micromobility. What is micromobility? Micromobility arises due to the inexorable push in current IP networks to have wireless access. Because of the proliferation of laptops and palmtop devices, it is inevitable that *wireless* access to an IP network will become the norm rather than the exception. Figure 7 shows an IP network with wireless access. The global IP networks (such as the Internet), are connected to the wireless access networks via gateways G1 and G2. Within the wireless access networks, there are wireless access points, b1 - b6, or more simply, base stations. These base stations serve the mobile hosts in a given wireless access network. It is movement *within* any one of the wireless access networks that constitutes micromobility, and movement *between* wireless access networks constitute macromobility.

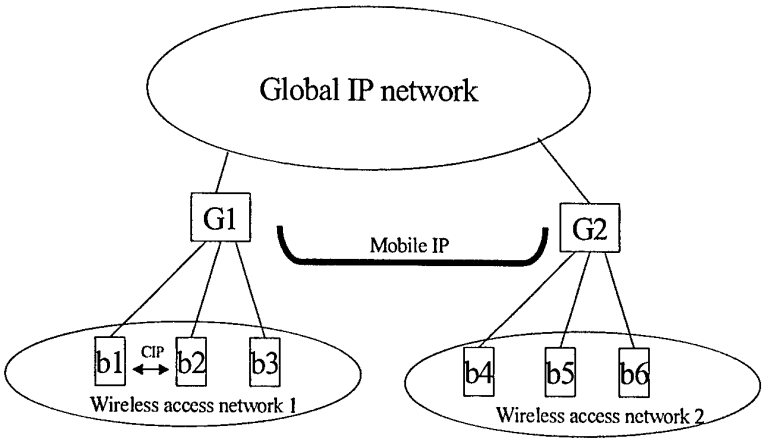

Figure 7:Architecture giving rise to micromobility

Mobile IP is not a suitable solution to handle the problem of micromobility. This is because of the inherent latency in the protocol that a mobile host has to undergo when changing networks. Recall that, in Mobile IP, when a mobile host changes subnet, it has to find a foreign agent, and also register with a (possibly distant) home agent. All this consumes valuable time so that the handover is not very fast. Now, within a wireless access network there may be many mobile hosts. Furthermore, cell sizes are made small in order to handle the number of hosts, and therefore, host migration between cells will be faster. This results in fast handovers, thereby necessitating very efficient location management procedures. Since Mobile IP is not optimised for this situation, there are other solutions that have been developed. The most prominent ones are Hawaii, Thema, SIP and Cellular IP. All these protocols are expected to co-exist with Mobile IP, in the sense that Mobile IP will be used to handle the problem of macromobility, and any one of the above mentioned protocols will be used to handle the problem of micromobility. None of these protocols have been

standardised, and at this stage, it is unclear as to which of these will be used as a standard, or, indeed, whether all four will be used. However, the solution developed by Columbia University, which is Cellular IP, has been gaining attention in the literature, so the discussion that follows will be about Cellular IP.

Cellular IP is an attempt to introduce the concepts of cellular telecommunications into what is, in the main, an IP related problem. This is especially true in the area of location management. Consider, for example, the registration procedure in Mobile IP. The mobile host sends registration requests at regular intervals even when it is idle, that is, when there is no active data transfer. This only serves to increase the traffic load in the network. This is not suitable in a wireless access network where a few base stations may be servicing many mobiles. When the mobile is idle, what is needed is minimum traffic and processing load on the wireless access network. Cellular IP guarantees this with its very efficient location management functions. Although details are beyond the scope of this report, it may be mentioned that these location management schemes are similar to those used in cellular telecommunications networks, that is, the existence of a coarse paging scheme and a much finer routing update scheme. Furthermore, the location management schemes in Cellular IP can be made to be dependent on the host migration frequency, by changing configuration parameters. All these techniques result in Cellular IP being able to support very fast handovers.

Although Cellular IP borrows from the concepts of cellular telecommunications, it is very much an IP solution. It is fully compatible with any network that uses IP, and can be interfaced as such. It uses three control packets and all of them are datagrams involving IP options. Unlike cellular telecommunications networks, it has no connection establishment phase. So, Cellular IP is appropriate for non guaranteed datagram delivery and best effort traffic. However, any future solutions to enhance QOS (Quality of Service) in IP networks could be applied to Cellular IP.

So, what are the market trends for Cellular IP and, indeed, the other protocols that are designed to handle micromobility? So far, the interest has been from academic institutions and the IETF. The IETF, in particular, is well aware of the importance of these solutions and there are many Internet Drafts that have been published. It is perhaps a matter of time before the ISPs begin to realise the importance of these protocols and the challenge that is inherent to cellular carriers. An attempt may be made to depict this challenge by interpreting user needs. When a user is travelling in a car or a high speed train, they might wish to maintain an ftp or telnet session. Maybe they might even be engaged in an active conversation over an IP phone. This would attack the very core of cellular telecommunications, namely voice delivery. This situation would arise provided that IP telephony is able to guarantee voice quality similar to that of current cellular networks.

4. Data in the Cellular World

Although this report is on mobility in IP networks, it is important to consider cellular networks as well. This is because cellular networks are being increasingly used to transmit data and to interface to IP networks. This method of providing mobility should be considered due to the large established subscriber base, and also the use of the existing infrastructure. The next generation of cellular networks will be the third generation. The first generation consisted of analogue systems such as AMPS (Advanced Mobile Phone Service) which were operational in the early 80s. Then came the second generation of digital systems with higher capacity and increased security features. These were rolled out in the early 90s and are still operational. The most prominent system is GSM (Global System for Mobile communications), which has now become a *de facto* standard. The future third generation systems will provide high data rate services such as multimedia services, will be world standards, and will consist of evolved packet switched networks.

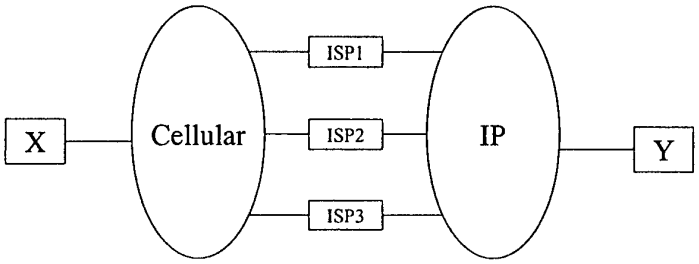

Figure 8:IP Mobility via cellular data

Indeed, at present, the packet switched data transmission system allied to GSM called GPRS (General Packet Radio Service) is being rolled out, and this is sometimes referred to as the 2.5th generation. An example of a third generation system is UMTS (Universal Mobile Telecommunication System) which is a European initiative.

Mobility in IP networks may be achieved with the aid of a cellular network. The simplest possible architecture for this is given in Figure 8. This architecture assumes that the cellular network operates in its normal sense as a circuit switched network. (Note that there are other possible architectures when packet switched networks such as GPRS are used). In the scenario given in Figure 8, X is could be a laptop or a personal digital assistant, which is attached to a mobile phone. Y is a remote host on an IP network, say, the Internet. The mobile phone at X is attached to the cellular network. The cellular network and the IP network are interfaced at various ISPs (Internet Service Providers). There are gateways at these ISPs which do the interfacing. The laptop at X and the node at Y of course have IP addresses. When Y desires to communicate with X, it does so via IP packets with the destination address pointing to X. This undergoes the normal IP routing methods and arrives at one of the ISPs. The ISPs see the entire cellular network as a single

IP subnet which serves hosts in a circuit switched manner. So, the relevant ISP makes a data call to the mobile phone at X and the data (circuit switched) is transmitted to X. The reverse process is observed when X desires to communicate with Y. So, the mobility for the node X is completely provided by the cellular networks. This, of course, means that the call is subject to the billing procedures of the cellular network, which are expensive, especially if the user is roaming away from home. Furthermore, most second generation cellular networks offer only a low speed connection (typically 9.6 kbit/s) on its circuit switched data connections. So, it is not foreseen that this method of obtaining mobility in IP networks will be very popular in the future.

4.1 CDPD (Cellular Digital Packet Data)

CDPD stands for Cellular Digital Packet Data, and is a U.S. initiative. This is a packet switched system that is overlaid on a cellular infrastructure, and as such, is quite different from the system mentioned at the beginning of this section. CDPD uses IP as its packet protocol. This system is operated in the 850 MHz. frequency band and uses the same frequencies as AMPS. So, the 30 kHz wide AMPS channels are used to transmit data whenever they are available, that is, when they are not occupied in an AMPS voice call. The gross data rate is 19.2 kbit/s. However, due to the overheads, such as error correction and synchronisation, the user data rate is deemed to be about 10 kbit/s, so this is in the same order as a circuit switched data system. One major difference is in the billing since, being a packet switched network, the charges are dependent on the amount of data transferred and not on the call duration. CDPD is backed by major U.S. cellular companies such as GTE and McCaw. However, the coverage so far has been in limited areas in the U.S., and being a link layer solution to the problem of mobility, the service is dependent on coverage. So, although fairly popular, CDPD is not expected to become an international standard.

4.2 GPRS (General Packet Radio Service)

The General Packet Radio Service (GPRS) is a packet switched network that is overlaid on a circuit switched network. GPRS is allied to GSM in that it uses extensions to the GSM infrastructure, but is completely autonomous in its operation. It is supposed to increase the range of circuit switched data services offered by GSM. Data services with bit rates upto 170 kbit/s are envisioned. Most of the Internet services such as file transfer, web browsing and e-mail are available as GPRS services. The high bit rate even allows compressed video to be transmitted with advanced compression algorithms.

GPRS supports many packet data protocols, such as IP and X.25. As such, it interworks with IP networks such as the Internet, and provides the possibility of mobility for hosts accessing these systems. GPRS terminals will have a phone number and an IP address. The phone number is used to make voice calls in the circuit switched GSM system and for translational purposes in GPRS, while the IP address is used for routing purposes in the packet switched GPRS network. Simultaneous calls are possible from a GPRS terminal. This means, for example, that a voice call may be initiated while a file transfer is

continuing in the background. However, this, of course, depends on the available bandwidth.

As mentioned before, GPRS interworks with IP networks. One of the services offered is a connectionless service with datagrams. However, GPRS also exhibits characteristics of the circuit switched world in that it provides for a variable Quality of Service (QOS), depending on the service requirements. Different QOS characteristics such as throughput and delay may be negotiated by the service provider and subscriber. However, to be fully effective the QOS characteristics of the interfacing IP network must be similar. To effect routing, two GPRS Support Nodes (GSNs) are defined. These are the GGSN and the SGSN, which correspond, respectively, to the home agent and foreign agent in Mobile IP. There is also a GPRS register (GR), which is similar to the Home Location Register (HLR) in GSM, in that it is a database which stores mappings from, for example, a phone number to an IP address. This is the totality of extensions used in a GPRS network.

GPRS networks are being rolled out now. The data services offered are relatively cheap compared to similar services offered in the circuit switched GSM. This is, of course, to be expected since data transmission is more conducive to packet switched networks. It remains to be seen as to how effective and popular these systems will become. This would determine the extent to which coverage is supplied, which would, in turn, affect the popularity. It is a feedback system.

4.3 WAP (Wireless Application Protocol)

WAP stands for Wireless Application Protocol, and is the new buzzword in wireless networks. However, it must be pointed out at the outset that WAP is not a mechanism for providing mobility for IP or other data networks. Rather, it is an application environment that consists of higher layer (layer 4 and above) protocols that are optimised for use in the wireless environment. WAP protocols operate on top of a large number of wireless networks including CDPD and GSM. So, the entities that provide the mobility are the networks such as CDPD and GSM, while WAP protocols optimise the operation of IP networks such as the Internet in the wireless environment. Indeed, WAP may be used on top of Mobile IP as well.

WAP uses many lower layer Internet protocols such as IP. As for the higher layer protocols such as the Transfer Control Protocol (TCP), Hyper Text Markup Language (HTML) and Hyper Text Transfer Protocol (HTTP), WAP uses its own modifications such as the Wireless Markup Language (WML). These modified protocols take into account the long latencies, low bandwidth, intermittent connectivity, and other vagaries of the wireless environment, and are optimised for use in these environments. Not only are the WAP protocols optimised for the wireless environment, but the WAP applications are optimised to be used with small handheld mobile terminals. For example, WAP has a micro browser that operates well with the small screens to be found in current mobile terminals. The current generation of small wireless devices are suitable for the inclusion of

WAP functionality, with possibly a small increase in memory. These terminals are known as WAP enabled devices.

All the WAP related design issues are handled by a body known as the WAP forum. Originally, the WAP forum consisted of Ericsson, Motorola, Nokia and Unwired Planet, but now there are over 90 members from all facets of the relevant industries. It is a very powerful body and the protocols developed under the guise of the WAP forum will inevitably become *de facto* standards. Furthermore, a large number of developers are willing to write WAP applications due to the strength of the WAP forum. WAP version 1.1 was adopted in May 1999, and WAP enabled products have now been released into the market. All indications are that WAP enabled devices will be very popular and will grow to have a big subscriber base in the future. However, as for providing mobility, as mentioned before, one has to look elsewhere.

5. Conclusions

This paper has been concerned with techniques for the provision of mobility in IP networks. The particular technique that has been standardised by the IETF is Mobile IP, which exists as Mobile IPv4 and Mobile IPv6. Although Mobile IPv6 is technically superior, it is not yet a full standard, and it has few implementations. Mobile IPv4 has been implemented on various platforms including Solaris, Linux and Windows NT. So far, deployment has been in academic network environments. However commercial organisations are becoming increasingly interested in Mobile IP, and deployment in commercial networks is bound to follow.

Mobile IP is not without its limitations. Specifically, it is not optimised for operation in the midst of fast handoffs. Many solutions to this problem have been put forward, and the protocol which seems to be gaining the most popularity is Cellular IP. Cellular IP is envisaged to be operated with Mobile IP, each of the two protocols addressing those parts of the environment for which they are optimised. Although a fully specified protocol, Cellular IP is yet to be sought after by commercial organisations. The IETF, however, is fully aware of its usefulness and functionality.

The final method for providing mobility in IP networks is to use cellular networks for the provision of mobility. This has the advantage that the networks and infrastructure are well established, and hence would take less effort to deploy. At present, cellular carriers have the ability to interface with IP networks. The disadvantage is the low data rates and high call costs associated with transferring data on a circuit switched network. The other disadvantage is the dependency on the link layer. A partial remedy to this problem has been found in the introduction of GPRS, which is a packet switched overlay on a GSM network. GPRS is currently being rolled out and it is still unclear as to what its market penetration rate would be.

6. ADDENDUM

There have been some changes since this paper was written. The following statements reflect the current situation in February, 2003.

- MIPv6 is still in the stage of an Internet Draft. There are very few implementations.
- The micromobility protocols have yet to be standardised.
- Cellular IP is still seen as the main protocol that addresses fast mobility. However, there has been no widespread deployment by industry. This may be attributed to the natural inertia that accompanies paradigm shifts.
- Cellular carriers have recognised Mobile IP as the prime method for provision of mobility in an IP network.
- GPRS systems have been rolled out. Coverage is about 95% of the coverage of GSM systems. However, the subscriber base is still very low.
- WAP is now fairly well established, and the subscriber base is growing.

It should be noted that these changes do not affect the assessments and conclusions given in the paper.

7. References

1. Perkins, C., "Mobile IP: Design Principles and Practice", Addison-Wesley, 1998.
2. Solomon, J., "Mobile IP: The Internet Unplugged", Prentice Hall, 1998.
3. Valko, A.G., "Cellular IP: A New Approach to Internet Host Mobility", Computer Communication Review, pp. 50-65, January 1999

DISTRIBUTION LIST

IP Convergence in Global Telecommunications
- Mobility in IP Networks

Sana Jayasinghe

AUSTRALIA

DEFENCE ORGANISATION

Task Sponsor

Director General C3I Development
DCD
DOISD
PD JP 2047 (CWAN)
PD JP 2068 (NOC)
PD JP 2061 (EXC3ITE)

S&T Program

Chief Defence Scientist
FAS Science Policy
AS Science Corporate Management
Director General Science Policy Development
} shared copy

Counsellor Defence Science, London (Doc Data Sheet)
Counsellor Defence Science, Washington (Doc Data Sheet)
Scientific Adviser to MRDC Thailand (Doc Data Sheet)
Scientific Adviser Joint
Navy Scientific Adviser (Doc Data Sheet and distribution list only)

Scientific Adviser - Army (Doc Data Sheet and distribution list only)

Air Force Scientific Adviser
Director Trials

Information Sciences Laboratory

Chief of Information Networks Division
Research Leader Military Information Networks
Head Network Requirements
Head Network Architecture
Head Wireless Systems
Research Leader Secure Communications
Head Intelligent Networks
Research Leader Military Computing Systems Branch
Sana Jayasinghe

DSTO Library and Archives

Library Edinburgh
Australian Archives
Library Canberra (Doc Data Sheet only)

Capability Systems Staff
Director General Maritime Development (Doc Data Sheet only)
Director General Aerospace Development (Doc Data Sheet only)

Knowledge Staff
Director General Command, Control, Communications and Computers (DGC4) (Doc Data Sheet only)

Navy
SO (SCIENCE), COMAUSNAVSURFGRP, NSW (Doc Data Sheet and distribution list only)

Army
ABCA National Standardisation Officer, Land Warfare Development Sector, Puckapunyal (4 copies)
SO (Science), Deployable Joint Force Headquarters (DJFHQ) (L), Enoggera QLD (Doc Data Sheet only)

Intelligence Program
DGSTA Defence Intelligence Organisation
Manager, Information Centre, Defence Intelligence Organisation

Defence Libraries
Library Manager, DLS-Canberra (Doc Data Sheet only)
Library Manager, DLS - Sydney West (Doc Data Sheet Only)

UNIVERSITIES AND COLLEGES
Australian Defence Force Academy
Library
Head of Aerospace and Mechanical Engineering
Serials Section (M list), Deakin University Library, Geelong, VIC
Hargrave Library, Monash University (Doc Data Sheet only)
Librarian, Flinders University

OTHER ORGANISATIONS
National Library of Australia
NASA (Canberra)

OUTSIDE AUSTRALIA

INTERNATIONAL DEFENCE INFORMATION CENTRES
US Defense Technical Information Center, 2 copies
UK Defence Research Information Centre, 2 copies
Canada Defence Scientific Information Service, 1 copy
NZ Defence Information Centre, 1 copy

ABSTRACTING AND INFORMATION ORGANISATIONS
Library, Chemical Abstracts Reference Service
Engineering Societies Library, US

Materials Information, Cambridge Scientific Abstracts, US
Documents Librarian, The Center for Research Libraries, US

INFORMATION EXCHANGE AGREEMENT PARTNERS
Acquisitions Unit, Science Reference and Information Service, UK

SPARES (5 copies)

Total number of copies: **49**

Page classification: UNCLASSIFIED

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

IP Convergence in Global Telecommunications
- Mobility in IP Networks

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Sana Jayasinghe

5. CORPORATE AUTHOR

Information Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-1393	AR-012-593	Technical Report	February, 2003

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
-	JTW 02/099	DGC4	28	3

13. URL on the World Wide Web

http://www.dsto.defence.gov.au/corporate/reports/DSTO-TR-1393.pdf

14. RELEASE AUTHORITY

Chief, Information Networks Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DEFTEST DESCRIPTORS

IP mobility, communications networks, computer networks, network connectivity

19. ABSTRACT

The paper describes the main techniques for providing mobility in an IP network. Towards this end the Mobile IP protocol is described in both its guises, namely MIPv4 and MIPv6. Fast mobility is addressed in the next section, and Cellular IP is chosen as the representative protocol. Then, the methods of providing mobility by using a cellular network is presented, and the paper concludes with the description of some common wireless standards.